REMARKS:

In the outstanding Office Action, the Examiner rejected claims 1-9. Claims 1 and 5-9 have been amended, claim 2 has been canceled without prejudice, and new claims 10-12 have been added. Thus, claims 1 and 3-12 remain pending for reconsideration which is requested. No new matter has been added. The Examiner's rejections are traversed below.

REJECTION UNDER 35 U.S.C. §102(b):

In the outstanding Office Action, claims 1-9 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,757,920 ('920).

'920 discusses a logon certification method in a distributed system where a secure package with a certified credential information is provided for each computer at a respective home domain and is used for connection outside the home domain.

The present invention enables a user to receive any one of a plurality of services by presenting common certificate information with a common certification number without requiring disclosure of identification and/or password data set correspondingly with available services other than the service the user is to receive.

The Examiner compares the '920 method for supporting roaming users/machines in a distributed system environment by providing logon certificates stored in respective domain controllers of the users/machines home domain with the present invention. In '920, each domain includes a domain controller holding logon certificate information about users for which the domain is the home domain (see, column 4, lines 46-49 and column 5, lines 10-14 of '920). The logon certificates have credentials of the users regarding connection to non-home domains (see, column 5, lines 14-17 of '920), and are provided to the users each time the users logon to the users' home domain to be later used to logon at a site in a different domain (see, column 6, lines 46-62 of '920). Thus, when a user logon using the logon certificates, the user is outside the user's domain where no information about the user is maintained (see, column 9, lines 20-23 of '920). This means that the logon certificates are provided from the home domains of the respective roaming users and are limited to allowing roaming access to the users.

The certifying method and system of the present invention allows users to access services requiring different identification and password information using common certificate information. As recited in amended independent claims 1 and 6-9, the present invention includes use of "... common certificate information in common with a plurality of services... " where it is determined "whether the certificate information of the user corresponds to the

common certificate information" and the user is allowed access of the plurality of services based on the determination. The present invention also includes, "storing identification information and password information for the particular service" based on which the user is certified and issued "the common certificate information" (see, amended independent claims 1 and 5-9 of the present invention). This enables a user to access a plurality of services that require input of respective identification and password information by using the common certificate information without requiring disclosure of the identification and password information to the other services.

For example, various service providers that offer services require corresponding password and/or identification information to access the services provided. The present invention stores "identification information and password information for a particular service" based on which the user is certified and issued "the common certificate information". The user is then permitted "to utilize the particular service when the certificate information of the user corresponds to the common certificate information" (see, amended independent claims 1 and 5-9 of the present invention). This allows the user to utilize the common certificate information to access all of the services of the service providers without the burden of having to memorize and input respective password and identification information of required by the service providers. The '920 method merely allows roaming of users within a distributed network where the user is allowed access to another domain based on preset logon certificate information located at the user's home domain.

It is submitted that the independent claims are patentable over '920.

For at least the above-mentioned reasons, claims depending from independent claims 1 and 5-9 are patentably distinguishable over '920. The dependent claims are also independently patentable. For example, as recited in claim 3, the certificating system includes "an invalidating device for invalidating the common certificate information when said certifying device has successfully certified the user". The '920 method does not teach or suggest, "invalidating the common certificate information" subsequent to certification of the user based on the identification and the password information.

Therefore, withdrawal of the rejection is respectfully requested.

NEW CLAIMS:

New claim 10 is added to emphasize that the method of the present invention includes, "receiving certificate information input by a user and determining whether the certificate information input by the user corresponds to the common certificate information" and "prompting

the user to indicate whether use of the common certificate information with the particular service should be prohibited upon validating use of the particular service with the presented common certificate". This allows the user to selectively opt out from using the common certificate information in relation to a particular service.

New claims 11 and 12 are added to highlight an aspect of the present invention where the method comprises "generating user information management table having the respective identification and password information of the plurality of service servers for each user" and "linking the common certificate information to each of the plurality of services upon authentication of a user based on respective password and identification information of the plurality of services". This enables "issuing the common certificate information in relation to each the plurality of service servers upon authenticating the user based on user's input of the respective identification and password information of the plurality of service servers" such that the user is authorized to use the plurality of services based on the common certificate information without the need to enter respective password and identification information of the plurality of services.

It is respectfully submitted that the '920 method does not teach or suggest the features of new claims 10-12.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 8/25/04

By: _____

J. Randall Beckers
Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE UNDER 37 CFR 1.8(a)
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on August 25th, 20 04
STAAS & HALSEY
By: Tammie Apework
Date: 8/25/04